

International Journal of Quantum Information
© World Scientific Publishing Company

Orthogonal-state-based cryptography in quantum mechanics and local post-quantum theories

S. Aravinda

*Poornaprajna Institute of Scientific Research,
4 Sadashivnagar Bangalore, India
aru@poornaprajna.org*

Anindita Banerjee

*Bose Institute, Centre of Astroparticle Physics and Space Science, EN Block, Sector - V, Salt
Lake, Kolkata, India
aninditabanerjee.physics@gmail.com*

Anirban Pathak

*Jaypee Institute of Information Technology, A-10, Sector-62, Noida, India
anirban.pathak@jiit.ac.in*

R. Srikanth

*Poornaprajna Institute of Scientific Research,
4 Sadashivnagar, Bangalore- 560080, India
srik@poornaprajna.org*

We introduce the concept of cryptographic reduction, in analogy with a similar concept in computational complexity theory. In this framework, class A of crypto-protocols reduces to protocol class B in a scenario X , if for every instance a of A , there is an instance b of B and a secure transformation X that reproduces a given b , such that the security of b guarantees the security of a . Here we employ this reductive framework to study the relationship between security in quantum key distribution (QKD) and quantum secure direct communication (QSDC). We show that replacing the streaming of independent qubits in a QKD scheme by block encoding and transmission (permuting the order of particles block by block) of qubits, we can construct a QSDC scheme. This forms the basis for the *block reduction* from a QSDC class of protocols to a QKD class of protocols, whereby if the latter is secure, then so is the former. Conversely, given a secure QSDC protocol, we can of course construct a secure QKD scheme by transmitting a random key as the direct message. Then the QKD class of protocols is secure, assuming the security of the QSDC class which it is built from. We refer to this method of deduction of security for this class of QKD protocols, as *key reduction*. Finally, we propose an orthogonal-state-based deterministic key distribution (KD) protocol which is secure in some local post-quantum theories. Its security arises neither from geographic splitting of a code state nor from Heisenberg uncertainty, but from post-measurement disturbance.

Keywords: quantum communication using orthogonal states, QSDC, QKD, quantum cryptography, cryptography in post-quantum theories

1. Introduction

A protocol of secure quantum key distribution (QKD) was proposed in 1984 by Bennett and Brassard¹. Since then several other QKD protocols have been proposed^{2,3,4,5,6,7,8}, and the notion of security has been considerably refined and strengthened. It is now established that QKD is unconditionally secure, while by contrast any classical cryptographic protocol is secure only under some assumptions about the hardness of performing some computations. This important feature (unconditional security) of QKD drew the attention of the cryptography community. However, all the initially proposed protocols of secure quantum communication^{1,2,3,4} were based on conjugate coding (i.e., encoding bits using non-orthogonal quantum states), and the applicability of these initial protocols was limited to QKD. It was soon realized that quantum resources can be used to implement other cryptographic tasks and that it is possible to construct protocols of secure quantum communication using orthogonal states.

Specifically, on the one hand, conjugate-coding-based protocols were proposed for quantum secure direct communication (QSDC)^{a 9,10,11}, quantum secret sharing¹², quantum dialogue^{13,14} etc. while on the other hand, a few protocols with orthogonal-state-based quantum cryptography were proposed^{5,6,7}. As in the case of conjugate-coding-based protocols, the initial protocols of orthogonal-state-based quantum communication^{5,6,7,15,16} were also limited to QKD.

To be precise, in 1995, Goldenberg and Vaidman⁵ proposed first orthogonal-state-based protocol for deterministic QKD (called GV). In 1997, Koashi and Imoto¹⁷ generalized the GV protocol and proposed a protocol similar to GV protocol, but which obviates the random sending time, a strict requirement of the original GV. Subsequently, in 1999 Guo and Shi⁶ proposed an orthogonal-state-based protocol of QKD which was based on the principle of quantum mechanical interaction-free measurement¹⁸. Recently, in 2009, Guo and Shi's idea was extended to a sophisticated orthogonal-state-based counterfactual QKD protocol by Noh⁷, which is now famously known as N09 or the counterfactual protocol of QKD. Later on, in 2010 Sun and Wen have proposed a modified N09¹⁶ which is more efficient than N09.

All these orthogonal-state-based protocols^{5,6,7,15,16} that were proposed between 1995 to 2010 were only theoretical ideas and limited to QKD. The interest on these protocols considerably increased in the recent past as several experimental realizations of orthogonal-state-based protocols of QKD were reported between 2010 to 2012^{19,20,21,22,23}. Motivated by these developments, in last two years,

^aIn a QKD protocol, a key is distributed first using quantum resources and then the key is used later for encryption of a message, whereas no such intermediary key is required in QSDC, which uses quantum resources to enable legitimate users to communicate directly without establishing a key. Further, a QSDC scheme does not require any classical communication for decoding of the information. There exists another class of schemes for direct secure quantum communication (i.e., quantum communication without an intermediary generation of key) which require additional classical information for decoding of the encoded information. Such schemes are referred to as deterministic secure quantum communication (DSQC).

some of the present authors extended the existing protocols of orthogonal-state-based QKD to obtain orthogonal-state-based protocols for quantum key agreement (QKA)²⁴, QSDC^{25,26}, DSQC²⁷, counterfactual certificate authentication²⁸, etc.

In most of our recent works on orthogonal-state-based secure quantum communication, we have used multi-qubit states and block transmission after applying a permutation operator Π on the qubits to be transmitted. Specifically, Π scrambles the order of particles. This procedure of permutation of particle (PoP) was first introduced by Deng and Long in 2003²⁹ to propose a protocol of “controlled order rearrangement encryption” (CORE). A detailed description of this technique and a short review of the orthogonal-state-based protocols that use this technique can be found in Refs.^{30,31}. Our recent works using PoP and multipartite orthogonal states suggest that any cryptographic task that can be performed using conjugate coding can also be performed by solely using orthogonal states³⁰.

This observation in general and successful construction of orthogonal-state-based QSDC^{25,26} protocol in particular lead to a couple of questions: (i) How is the security of QSDC protocols connected to that of QKD protocols? (ii) Is it possible to design orthogonal-state-based protocols of secure quantum communication in local post-quantum theories (say, in generalized local theory (GLT), generalized probabilistic theory (GPT) or in a generalized non-signaling theory (GNST))³²? (iii) Is it possible to design orthogonal-state-based quantum device independent protocols of QSDC and QKD.

The present paper aims to answer the first two questions. In what follows, we answer the first question and show that we can construct a QSDC scheme by replacing qubit streaming in a QKD scheme with block-encoding of qubits. This reduces the security proof of the QSDC scheme to the security proof of the QKD scheme, in the sense that if the QKD scheme is secure, then so is the QSDC scheme built on top of it using PoP. This reduction scheme is referred to as *block reduction*. Similarly, it is shown that the security proof of a QKD scheme reduces to that of a QSDC scheme, in the sense that if we have a secure QSDC scheme, then we can always distribute a random key in a secure manner using that scheme. This reduction procedure is referred to as *key reduction*. Further, we answer the second question by providing an orthogonal-state-based deterministic QKD protocol which is secure in some post-quantum theories (namely in GPT, GLT or the local part of GNST) and note that security of the orthogonal-state-based protocol valid in post-quantum theories arises not from uncertainty, but from post-measurement disturbance.

The remaining part of the paper is organized as follows. In Section 2, we introduce the idea of cryptographic reduction, inspired by a similar idea in computability and complexity theory, whereby the security of a class of protocols is derived from another related to it by means of a secure transformation. In Section 2.1 we describe one of the two kinds of reductions considered here: *block reduction*, while in Section 2.2 we study a reduction in the opposite direction, called *key reduction*.

In Sec. 3, we show that orthogonal-state-based protocols of secure communication can be designed in local post-quantum theories, too. Specifically, the possibility of orthogonal-state-based secure communication in a GLT and in local part of a GNST is established. Finally we conclude the paper in Sec. 4.

2. Cryptographic Reduction

The concept of reduction in computability theory and complexity theory is a basic tool by which the (efficient) (un)solvability of different problems can be comparatively deduced. For example, the *Turing reduction* from problem A to problem B can be regarded as an algorithm to solve A , assuming that an algorithm to solve B is given. In complexity theory, *Cook reduction* from problem A to B is a polynomial-time algorithm that efficiently solves instances of problem A given an oracle that solves B in a single time-step.

A comparison of QSDC and QKD suggests that it is useful to define an analogous concept of reduction for cryptography. The cryptographic reduction in scenario X from crypto-protocols of class A to those of class B is a secure procedure X by which given a protocol a in class A , there is an instance b of class B , such that a has been created from b by using X , and a is secure if b is secure. We discuss two scenarios X below. In one, X represents the task of block encoding qubits, whereby a fixed number of qubits is taken as a block, re-arranged according to a random permutation, and then transmitted as a block; this gives block reduction from a QSDC class to a QKD class of protocols. Another scenario is one where X represents the substitution of a random bit string for a direct message; this gives key reduction, which works in the opposite direction to block reduction. These two reductions are discussed in the following two subsections.

2.1. Block reduction

In classical cryptography, block ciphers and stream ciphers are two frequently used algorithms for encryption. In the former, one employs a symmetric key to transform a block of fixed-length of bits. For example, the key may scramble the bits according to a certain permutation. By contrast, a stream cipher combines individual bits or bytes of a plaintext message with a random key stream. By default, QKD employs the sequential streaming of individual qubits or entangled states, while QSDC conventionally employs the manipulation of blocks of qubits by re-arranging the particles, and then transmitting those blocks of qubits en bloc.

Recently it was shown how the use of block transmission and an order-rearrangement technique can make an orthogonal-state based deterministic two-qubit QKD protocol suitable for QSDC²⁶. The QSDC protocol presented there: (a) Alice prepares $3N$ singlet states. Of these she applies a PoP scheme Π on N pairs together with $2N$ singlet halves. (b) She transmits these re-arranged $4N$ particles to Bob over an authenticated quantum communication channel. (c) After Bob acknowledges their receipt, she reveals the information to unscramble the N full

pairs transmitted to Bob, who measures these in the Bell basis to determine the error rate e by a public discussion with Alice. If the error rate is too high, they abort the protocol run. (d) Alice encodes a $2Nh(e)$ -bit message into a classical error correcting $[2N, 2Nh(e)]$ -code, and encodes this onto N of the remaining $2N$ qubits by quantum dense-coding. Here h is the Shannon binary entropy. Alice transmits these $2N$ qubits to Bob. (e) After Bob's acknowledgment, Alice identifies the check pairs, which are then used to confirm that the error rate remains not larger than e . Upon confirmation, Alice reveals the information that would allow Bob to pair the remaining N particles with their partner particles, in order that the message may be decoded.

A QKD scheme is secure if there is a real number e_0 such that $0 \leq e_0 \leq 1$ and the observed error rate e satisfies

$$e \leq e_0 \Rightarrow I(A : B) \geq I(A : E). \quad (1)$$

This ensures that if Eve is restricted only to attack the (memoryless) communication channel (and the devices and initial states, both of which are assumed to be well characterized), then Alice and Bob can extract some secret bits via key reconciliation and privacy amplification³³.

The idea behind Eq. (1) is essentially the information-vs-disturbance trade-off in quantum information theory. In a QKD protocol, Alice generates a random classical bit or dit (a d -level number) s_j . She encodes the bit (or dit) in an entangled state $|\phi^{(j)}\rangle_S$ and *streams* (i.e, sequentially transmits) N such entangled states to Bob. Eve prepares probe P_j in the initial state $|\psi\rangle_P$. When Alice's system S_j is transmitted towards Bob, Eve executes the interaction U between P_j and S_j , producing the entangled state

$$\rho_P^{(j)} = \text{Tr}_S [U^{\otimes N} (|\Phi\rangle_S |\Psi\rangle_P \langle\Phi|_S \langle\Psi|_P) U^{\otimes N\dagger}], \quad (2)$$

where $|\Phi\rangle_S = \bigotimes_j |\phi^{(j)}\rangle$ and $|\Psi\rangle_P = |\psi\rangle_P^{\otimes N}$. Based the subsequent classical communication between Alice and Bob, Eve measures $\rho_P^{(j)}$ in a suitable basis to extract information about s_j . Here U is optimal in the sense that it maximizes Eve's information about classical secret s_j for a given observed error rate e .

In the PoP-version (\mathcal{P}^Π) of a cryptography protocol \mathcal{P} , because the streaming is replaced with block-coding of qubits, Eve does not know during their transit which entangled particles are partnered with which. She replaces probes P_j and with a single master probe P' , and replaces U with U' , a unitary that interacts all N qubits with P' . Here the primes indicate corresponding quantities in \mathcal{P}' . Since the PoP-version is the same as the old protocol with particle re-arrangement, therefore to gain the same amount of information, Eve must generate a greater level of system-probe entanglement to accommodate the various permutation possibilities, and correspondingly effect greater channel noise. For any fixed $I(A:E) = I'(A:E)$, the error rate e' generated in the PoP version will be greater than e . Conversely, for a fixed error $e = e'$, we must have $I'(A:E) < I(A:E)$.

6 Aravinda, S. et al.

On the one hand, this means that the error threshold (e'_0) till which \mathcal{P}^Π remains secure as a QKD protocol will be larger, i.e., $e'_0 > e_0$. The quantitative determination of e'_0 will be an interesting, if difficult, question. On the other hand, if $e = e' = e_0$, then $I'(A:E) < I(A:E) = I(A:B) = I'(A:B)$. In fact, since there are exponentially many ways to permute N particles, $I'(A:E)$ vanishes rapidly as N increases^{26,29}. This can be expressed as the QSDC condition

$$e \leq e_0 \Rightarrow \lim_{N \rightarrow \infty} I(A:B) > I'(A:E) \approx 0, \quad (3)$$

which may be contrasted with the QKD condition (1). Since $I'(A:E)$ asymptotically vanishes, Alice can directly encode her message, allowing the sender to use a QSDC protocol instead of a QKD protocol.

Our result implies that given a QSDC protocol (\mathcal{P}^Π) obtained via replacing stream transmission by block transmission in a QKD protocol \mathcal{P} , then if \mathcal{P} is secure, so is \mathcal{P}^Π asymptotically at the threshold error rate determined by \mathcal{P} . Define by $\mathfrak{S}(\mathcal{P}^{\text{QKD}})$ the class of QKD protocols that transmit data from Alice to Bob using streaming of individual qubits or individual entangled states of qubits. Further define by $\mathfrak{S}(\mathcal{P}^{\text{QSDC}})$ the class of QSDC protocols derived therefrom using block coding. Thus to every QSDC protocol in this class, we can associate a corresponding protocol in $\mathfrak{S}(\mathcal{P}^{\text{QKD}})$, whose security guarantees that of the QSDC protocol. We represent this situation by:

$$\mathfrak{S}(\mathcal{P}^{\text{QSDC}}) \leq_B \mathfrak{S}(\mathcal{P}^{\text{QKD}}). \quad (4)$$

This deduction of the security of a class of QSDC protocols from a corresponding QKD class is block reduction. A reduction that works in the opposite direction is key reduction, which is described below.

2.2. Key reduction

Given a secure QSDC scheme \mathcal{P}^Π , it is obvious that it can be converted into a secure QKD scheme, by transmitting a random key instead of a message. Of course, we must assume that the key itself is truly random and not vulnerable to attacks like the known-plain-text attack, etc. Let the class of QKD protocols obtained from QSDC protocols in this way—by messaging a key—be denoted $\mathfrak{S}(\mathcal{P}^{\text{QKD}'})$. Thus to every QKD protocol in this class, we can associate a corresponding protocol in $\mathfrak{S}(\mathcal{P}^{\text{QSDC}})$, whose security guarantees that of the QKD protocol. We represent this situation, which works in the direction opposite to (4), by

$$\mathfrak{S}(\mathcal{P}^{\text{QKD}'}) \leq_K \mathfrak{S}(\mathcal{P}^{\text{QSDC}}). \quad (5)$$

Broadly, we interpret ' $\mathcal{A} \leq_K \mathcal{B}$ ' as the key-reducibility of protocol class \mathcal{A} to class \mathcal{B} , meaning that we obtain a secure instance of \mathcal{A} if the \mathcal{B} counterpart is secure and furthermore a secure random number generator is available.

With a slight modification, the above argument can be extended to a quantum key agreement (QKA) protocol²⁴. QKA is a quantum key distribution scheme in

which Alice and Bob must both contribute equally to the final key. Let $\mathfrak{S}(\mathcal{P}^{\text{QKA}'})$ denote the class of QKA protocols derived from QKD by a secure method X . For example, suppose that the final reconciled QKD key, of even length m , has only Alice's contribution. Then Bob publicly announces $\frac{m}{2}$ coordinates, chosen randomly by him. The final key is the secret bits in these locations. Clearly, if the QKD protocol is secure, then so is the derived QKA protocol. We can express this situation by

$$\mathfrak{S}(\mathcal{P}^{\text{QKA}'}) \leq_K \mathfrak{S}(\mathcal{P}^{\text{QSDC}}). \quad (6)$$

A QKA protocol need not be derived from a QKD protocol in this way, and in that case, such a protocol is not covered in $\mathfrak{S}(\mathcal{P}^{\text{QKA}'})$.

3. Deterministic key distribution in local post-quantum theories

GPT is an operational framework³² that allows us to comparatively describe a wide class of theories, including classical mechanics, quantum mechanics and post-quantum theories of the box-world type³⁴. Here 'operational' means that we do not concern ourselves with the state space (such as Hilbert space), but instead only with the vector space of probabilities that can be obtained by performing *fiducial* measurements on allowed states in a theory. A set of fiducial measurements $M = \{\mu = 0, 1, \dots, \mu = K\}$ is a minimal and sufficient set whose outcome statistics completely specify the state.

Therefore, a state in GPT is specified by the probability vector obtained under different fiducial measurements, $\mu = 0, 1, \dots, J$, with outcomes $\alpha = 0, 1, \dots, K$:

$$\vec{\mathbf{P}} = \begin{pmatrix} P(\alpha = 0|\mu = 0) \\ P(\alpha = 1|\mu = 0) \\ \vdots \\ \hline P(\alpha = 0|\mu = 1) \\ P(\alpha = 1|\mu = 1) \\ \vdots \\ \hline \vdots \end{pmatrix}, \quad (7)$$

where $P(\alpha = k|\mu = j)$ is the probability that measuring $\mu = j$ yields outcome $\alpha = k$. Normalization requires $\forall_j \sum_{\alpha=k}^J P(\alpha = k|\mu = j) = 1$.

In classical mechanics, any state can be specified with single fiducial measurement. For example, the state of a coin can be represented by the toss probabilities, as

$$\vec{\mathbf{P}} = \begin{pmatrix} P(\alpha = 0|\mu = 0) \\ P(\alpha = 1|\mu = 0) \end{pmatrix}, \quad (8)$$

where $P(\alpha = 0|\mu = 0)$ is the probability of getting $\alpha = 0$ (i.e., head), and $\mu = 0$ is the measurement implemented by tossing. As another example, a classical

particle requires specifying its position and momentum, but these two attributes can be considered as independent systems requiring a single fiducial measurement. By contrast, a (scalar) *quantum* particle requires two fiducial measurements: position and momentum.

By measuring a qubit along X , Y , and Z direction, the state of a qubit can be fully represented, making these as three fiducial measurements for the state space of qubits in quantum mechanics. For example, the qubit with spin-up in the Z direction can be described by

$$\vec{P} = \begin{pmatrix} P(0|X) \\ P(1|X) \\ \frac{P(0|Y)}{P(1|Y)} \\ \frac{P(0|Z)}{P(1|Z)} \end{pmatrix} = \begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \\ \frac{1}{2} \\ 1 \\ 0 \end{pmatrix}, \quad (9)$$

where $P(0|X)$ is the probability of obtaining spin up by measuring in the X direction, and so on.

We note that \vec{P} in Eq. (9) corresponds to a pure state in quantum mechanics. Now consider a local post-quantum theory— a GLT— with three fiducial measurements but a larger state space, in which pure states \vec{P} have the form (9) and $P(\alpha = k|\mu = j)$ is 0 or 1. A pure qubit is represented a mixture of such GLT pure states. A state in this GLT is called a *gbit* (for ‘generalized bit’).

The gbit can quite generally be of the type J -in- K -out, i.e., one with J fiducial measurements, each with K outcomes. Obviously, qubit is related most closely to a 3-in-2-out gbit. Let us consider a 2-in-2-out gbit, whose pure states are:

$$g_0 = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}; \quad g_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}; \quad g_2 = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}; \quad g_3 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}, \quad (10)$$

where the upper (lower) pair refers to the state in fiducial property ‘ X ’ (‘ Z ’).

An arbitrary gbit for our purpose is a convex combination of the above four elements. For example, the ± 1 eigenstates of the qubit observable X would be *mixed* states of gbits:

$$|X+\rangle = \begin{pmatrix} 1 \\ 0 \\ \frac{1}{2} \\ \frac{1}{2} \end{pmatrix} := \frac{1}{2}(g_0 + g_1); \quad |X-\rangle := \begin{pmatrix} 0 \\ 1 \\ \frac{1}{2} \\ \frac{1}{2} \end{pmatrix} = \frac{1}{2}(g_2 + g_3). \quad (11)$$

A similar representation follows if we also include Y measurements in the picture, which we drop for simplicity.

Each of the above states may be considered orthogonal in the sense of pairwise distinguishability, i.e., there is a measurement that deterministically distinguishes

between any pair of them. E.g., g_0 and g_1 are distinguished by measuring Z , while g_0 and g_2 are distinguished by measuring X . These gbits lack Heisenberg uncertainty in that both X and Z can simultaneously take definite values. However, they admit *post-measurement disturbance*, whereby performing one fiducial measurement disturbs the statistics of the other fiducial measurements. For example, measuring X on a qubit prepared in the eigenstate of Z , disturbs the statistics of Z . A similar unbiased post-measurement disturbance is seen in gbits. For example, measuring X on g_2 deterministically returns $\alpha = 1$, but the post-measurement state will be an unbiased mixture of g_2 and g_3 . Quantum measurements have both uncertainty and post-measurement disturbance, while GPT states have only disturbance, and no uncertainty.

It was already known³² that a pair of nonlocally correlated gbits, which form a PR box³⁴, can be used for KD using a protocol like the Ekert protocol², and it was conjectured that this would be the case in any non-classical theory. The method we earlier used²⁶ to convert a deterministic QKD protocol with Bell states into a QSDC protocol by replacing streaming with block-coding, can be adapted to the post-quantum theories by replacing Bell states by PR boxes. Alice prepares a sequence of PR boxes that encode agreed-upon bits. She permutes the particles use a PoP configuration, and transmits the resulting particles to Bob. Bob decodes them after receiving the Π information.

We now show that in a GLT, gbits can be used as a basis for a deterministic GLT-KD (i.e., the GLT version of QKD). We may regard the pure states of the GLT ‘orthogonal’ if there is a fiducial measurement that distinguishes any pair of them in a single shot. This does not entail that the set of all pure states will be jointly distinguishable. More generally, our result applies to the local part of a GNST³². We now propose the following deterministic orthogonal-state-based GLT-KD protocol (which we call GLT-2S):

Encoding and Sending: Alice randomly and sequentially generates bit $x = 0$ or $x = 1$. In the former case, she transmits g_0 to Bob, while in the latter case, g_3 . Note that g_0 encodes bit $x = 0$ in both X and Z , while g_3 encodes bit $x = 1$ in both X and Z .

Bob’s receipt: Bob measures either X or Z in the received gbit states, to extract the encoded bit deterministically.

Computing error rate: Over a public channel, Alice and Bob estimate the error rate on the key so extracted. They publicly agree on certain coordinates of gbits and observables (X or Z) on those gbit coordinates. Bob announces the outcomes on those coordinates. If too many of them are mismatched, they abort the protocol.

Note that the coding in GLT-2S is not like conjugate coding in BB84 or B92, because there is no uncertainty between X and Z in GLT. For the same reason, while a public announcement of bases would be needed in BB84, here none is required, and furthermore, the raw bits generated are automatically the sifted bits. Since the

coding states are deterministically distinguishable, and in that sense orthogonal, GLT-2S may be considered as the post-quantum equivalent of the Goldenberg-Vaidman protocol (GV)⁵. On the other hand, a single gbit in GLT is spatially localized, making it similar to BB84 in this sense, rather than to GV.

In GLT-2S, what is remarkable is that security comes from post-measurement disturbance, and not from Heisenberg uncertainty. An eavesdropper Eve (limited by the theory to only be able to perform the stated fiducial measurements³⁵) can deterministically extract the encoded bit by measuring either X or Z , but she will disturb the other observable, which can be detected in the error detection step. If Eve measured n gbits in either X or Z basis, she extracts n bits of information, but she disturbs the other fiducial observable. If Bob measures that during the error check (which he does with probability $\frac{1}{2}$), he and Alice detect the attack with probability $\frac{1}{2}$. Thus, the probability that Eve can launch this attack and not be detected is $1 - \frac{1}{2} \cdot \frac{1}{2} = \frac{3}{4}$ per attacked gbit, which drops as $(\frac{3}{4})^n$ over n gbits. This exponential drop implies unconditional security against an Eve restricted to attacking single gbits. In Eq. (10), if instead we use a GLT with 3 fiducial measurements, and a similar GLT-KD with two states, this would be analogous to the six-state protocol³⁶, and Eve's corresponding probability to escape detection will fall faster, given by $p_{\text{esc}} = (\frac{2}{3})^n$. Generally, with a GLT where gbits are of the type J -in- K -out, $p_{\text{esc}} = (1 - \frac{J-1}{J} \frac{K-1}{K})^n$, indicating that in this sense a protocol is more secure in a theory with more fiducial measurements and outcomes.

4. Conclusions and discussions

Security in quantum cryptography has contributions from both Heisenberg uncertainty and post-measurement disturbance, while in GLT-2S, it comes only from disturbance. Intrinsic randomness, which lies at the heart of nonclassicality³⁷, can manifest both in uncertainty and post-measurement disturbance. Our work here suggests that only the randomness concerned with disturbance is essential to cryptographic security, though that concerned with uncertainty can quantitatively modify the secure limit.

Inspired by the analogous concept of reduction in computability theory and complexity theory, we introduced in this work the concept of cryptographic reduction. In particular, we defined block reduction of QSDC class of protocols to QKD class of protocol, and key reduction that works vice versa. These reductive methods can be used to understand the relationship between the security of these two types of crypto-tasks. In condition (3), since $I'(A:E)$ asymptotically vanishes, we expect that the condition will hold good even when e'_0 (the secure threshold for QSDC) drops well below the QKD threshold e_0 , and indeed, becomes arbitrarily small. A derivation of this will be interesting both practically and foundationally.

As far as we know, the protocol GLT-2S that we proposed here appears to be the first effort to design an (orthogonal-state-based) cryptographic protocol for a *local* post-quantum theory. Related work has been either about a post-quantum

non-signaling³⁸ or signaling³⁹ Eve attacking a quantum protocol, or a protocol in a post-quantum nonlocal theory⁴⁰. GLT-2S is interesting from a foundational perspective as it provides a clearer insight into the origin of security in quantum mechanics, without reference to nonlocality.

Acknowledgment: SA acknowledges support through the INSPIRE fellowship [IF120025] by the Department of Science and Technology, Govt. of India and Manipal university graduate programme. AP and RS thank the Department of Science and Technology (DST), India for support provided through the DST projects No. SR/S2/LOP-0012/2010 and SR/S2/LOP-02/2012, respectively.

References

1. Bennett, C. H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, 175-179 (1984)
2. Ekert, A. K.: Quantum cryptography based on Bell's Theorem. Phys. Rev. Lett. 67, 661-663 (1991)
3. Bennett, C. H.: Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett. 68, 3121-3124 (1992)
4. Gisin, N., Ribordy, G., Tittel, W., Zbinden, H.: Quantum cryptography. Rev. Mod. Phys. 74, 145-195 (2002)
5. Goldenberg, L., Vaidman, L.: Quantum cryptography based on orthogonal states. Phys. Rev. Lett. 75, 1239-1243 (1995)
6. Guo, G.-C., Shi, B.-S.: Quantum cryptography based on interaction-free measurement. Phys. Lett. A 256, 109-112 (1999)
7. Noh, T.-G.: Counterfactual quantum cryptography. Phys. Rev. Lett. 103, 230501 (2009)
8. S. Zhang, J. Wang and C.-J. Tang: Counterfactual Quantum Deterministic Key Distribution. Commun. Theor. Phys. 59 (2013) 27V31.
9. Boström, K., Felbinger, T.: Deterministic secure direct communication using entanglement. Phys. Rev. Lett. 89, 187902 (2002)
10. Lucamarini, M., Mancini, S.: Secure deterministic communication without entanglement. Phys. Rev. Lett. 94, 140501 (2005)
11. Cai, Q.-y., Li, B.-w.: Improving the capacity of the Boström-Felbinger protocol. Phys. Rev. A 69, 054301 (2004)
12. Hillery, M., Buzek, V., Bertiaume, A.: Quantum secret sharing. Phys. Rev. A 59, 1829-1834 (1999)
13. An, N. B.: Quantum dialogue. Phys. Lett. A 328, 6-10 (2004)
14. Shukla, C., Kothari, V., Banerjee, A., Pathak, A.: On the group-theoretic structure of a class of quantum dialogue protocols. Phys. Lett. A 377, 518-527 (2013)
15. Shenoy, A., Srikanth, R., Srinivas, T.: Semi-counterfactual cryptography, Europhys. Lett. 103, 60008 (2013)
16. Sun, Y., Wen, Q.-Y.: Counterfactual quantum key distribution with high efficiency. Phys. Rev. A 82, 52318 (2010)
17. Koashi, M., Imoto, N.: Quantum cryptography based on split transmission of one-bit information in two steps. Phys. Rev. Lett. 79, 2383-2386 (1997)
18. Elitzur, A. C., Vaidman, L.: Quantum mechanical interaction-free measurements. Found. Phys. 23, 987-997 (1993)
19. Traina, P., Gramegna, M., Avella, A., Cavanna, A., Carpentras, D., Degiovanni, I. P.,

12 *Aravinda, S. et al.*

- Brida, G., Genovese, M.: Review on recent groundbreaking experiments on quantum communication with orthogonal states. *Quantum Matter* 2, 153-166 (2013)
20. Avella, A., Brida, G., Degiovanni, I. P., Genovese, M., Gramegna, M., Traina, P.: Experimental quantum-cryptography scheme based on orthogonal states. *Phys. Rev. A* 82, 062309 (2010)
21. Ren, M., Wu, G., Wu, E., Zeng, H.: Experimental demonstration of counterfactual quantum key distribution. *Laser Phys.* 21, 755-760 (2011)
22. Brida, G., Cavanna, A., Degiovanni, I. P., Genovese, M., Traina, P.: Experimental realization of counterfactual quantum cryptography. *Laser Phys. Lett.* 9, 247-252 (2012)
23. Liu, Y., Ju, L., Liang, X.-L., Tang, S.-B., Tu, G.-L. S., Zhou, L., Peng, C.-Z., Chen, K., Chen, T.-Y., Chen, Z.-B., Pan, J.-W.: Experimental demonstration of counterfactual quantum communication. *Phys. Rev. Lett.* 109, 030501 (2012)
24. Shukla, C., Alam, N., Pathak, A.: Protocols of quantum key agreement solely using Bell states and Bell measurement. *Quant. Info. Process.* (2014) In Press, DOI: 10.1007/s11128-014-0784-0.
25. Shukla, C., Pathak, A., Srikanth, R.: Beyond the Goldenberg-Vaidman protocol: Secure and efficient quantum communication using arbitrary, orthogonal, multi-particle quantum states. *Int. J. Quant. Info.* 10, 1241009 (2012)
26. Yadav, P., Srikanth, R., Pathak, A.: Two-step orthogonal-state-based protocol of quantum secure direct communication with the help of order-rearrangement technique. *Quant. Info. Process.* (2014) In Press, DOI: 10.1007/s11128-014-0825-8
27. Shukla, C., Pathak, A.: Orthogonal-state-based secure direct quantum communication without actual transmission of the message qubits, *Quant. Info. Process* 13 (2014) 2099-2113
28. Shenoy, A., Srikanth, R., Srinivas, T.: Counterfactual quantum certificate authorization. *Phys. Rev. A* 89, 052307 (2014)
29. Deng, F.-G., Long, G. L.: Controlled order rearrangement encryption for quantum key distribution. *Phys. Rev. A* 68, 042315 (2003)
30. Shukla, C., Banerjee, A., Pathak, A., Srikanth, R.: Secure Quantum Communication with Orthogonal States. *arXiv:1407.3412* (2014)
31. Pathak, A.: Elements of quantum computation and quantum communication. CRC Press, Boca Raton, USA (2013)
32. Barrett, J.: Information processing in generalized probabilistic theories. *Phys. Rev. A* 75, 32304 (2007)
33. Csizár, I. and Körner, J.: Broadcast channels with confidential messages. *IEEE Trans. Inf. Theory*, 24, 339 (1978).
34. Popescu, S., D. Rohrlich, Quantum nonlocality as an axiom, *Found. Phys.* 24, 379-385 (1994).
35. O. C. O. Dahlsten, Andrew J. P. Garner and Vlatko Vedral. How uncertainty enables non-classical dynamics. *Nat. Commun.* 5:4592 (2014).
36. D. Bruss. Optimal eavesdropping in quantum cryptography with six states. *Phys. Rev. Lett.* 81, 3018 (1998).
37. Aravinda, S. and Srikanth, R.: Complementarity between signalling and local indeterminacy in quantum nonlocal correlations. *arXiv:1309.4435* (to appear in *Quant. Info. Comput.*)
38. Barrett, J., Hardy L., and Kent, K.: No Signaling and Quantum Key Distribution. *Phys. Rev. Lett.* 95, 010503 (2005).
39. Akshata Shenoy H., S. Aravinda, R. Srikanth, D. Home. Exploring the role of Leggett-Garg inequality for quantum cryptography. *arXiv:1310.0438*.
40. Pawłowski, M. Security proof for cryptographic protocols based only on the monogamy

of Bell's inequality violations. Phys. Rev. A 82, 032313 (2010).